Attorney Docket No. 9432-000129

MEASUREMENT-BASED ADMISSION CONTROL UTILIZING EFFECTIVE ENVELOPES AND SERVICE CURVES

BACKGROUND AND SUMMARY OF THE INVENTION

The present invention relates generally to network-based communication architecture. More particularly, the invention relates to providing controlled quality of service in packet-based networks through admission control.

Currently much of the Internet is designed to provide "best effort" service. The Internet Protocol (IP) is designed to deliver packets of information to an ultimate destination through any available internal links that enable delivery. The actual time it takes to deliver these packets depends on the route taken and the traffic congestion encountered in route. The original design of the Internet Protocol focused on providing ultimate delivery, with the actual time to achieve delivery being only a secondary consideration.

As the uses for the Internet have grown, and as Internet traffic has expanded geometrically, the original emphasis on delivery over timing is being challenged. With multicast applications and streaming audio and video applications growing in popularity, packet delivery time has become a central focus. Quality of Service (QoS) is a term often used to describe the degree to which a communications network provides reliability, availability and timely throughput. Quality of service addresses issues such as transmission speed, timeliness of packet delivery, amount of jitter a network introduces into packet streams, and the probability of outright packet loss. As businesses begin to rely

more and more on their Internet presence, some have expressed willingness to pay more for higher quality of service because the higher quality of service translates directly into a smoother, more responsive experience for their customers. Some Internet service providers thus offer different service level agreements through which they commit to provide different levels of service quality at different fee rates.

There are many proposals for improving quality of service in packet-switched networks such as the Internet. Quality of service may be improved at the individual router level by making the routers faster and more intelligent. However this also increases the system cost. Other proposals address the quality of service issue at the network model level. At the network model level, the performance of individual routers are largely ignored; focus instead shifts to the aggregate performance of all routers in the network. One popular approach is to consider the aggregate network only in terms of its outer boundary or end-to-end performance. Using such an analytical approach, the performance of the entire network, and the quality of service it provides, can be largely controlled by the behavior of the routers occupying the edge of the network (that is, the routers at the ingress and egress points).

There are several end-to-end network models for controlling quality of service (QoS) in popular use today. Among the leading models are *Integrated Services (IntServ)*, and *Multi-Protocol Label Switching (MPLS)* and *Differentiated Services (DiffServ)*. IntServ supports a per-flow quality of service guarantee. It employs a relatively complex architecture in which resources are reserved by means of a signaling protocol that sets up paths and reserves

resources. MPLS provides another quality of service guarantee approach that focuses on packet forwarding. Packets are assigned labels at the ingress of an MPLS-compatible domain. Subsequent classification, forwarding and services for the packets are then based on those labels.

Models, such as IntServ and MPLS, address QoS on a *per connection* basis and can present scalability difficulties. To provide better scalability, other models have been proposed that address QoS on a traffic *aggregate* basis. DiffServ is one example of such a model. DiffServ provides quality of service guarantees to packet aggregates by marking packets differently to create different packet classes/aggregates that are entitled to different quality of service handling.

For the most part, aggregate traffic-based network models share a number of common concepts. They begin from a premise that the network can be characterized as having edge and core routers. The edge routers accept customer traffic (i.e., packets from any source outside the network). Core routers provide transit packet forwarding services among other core routers and/or edge routers. The edge routers control ingress of traffic and thus perform an important *admission control* function, by permitting or declining requests by outside traffic to enter the network. With the ultimate traffic flow being controlled by the edge routers, through admission control, the core routers simply need to differentiate traffic insofar as necessary to cope with transient congestion within the network itself. The network models may employ statistical multiplexing to maximize utilization of the core router resources.

Predicting and controlling traffic flow through a network at the aggregate level is a very complex problem. Admission control algorithms that overly restrict ingress waste internal core router resources. On the other hand, admission control algorithms that are too lax can flood the network with too much traffic, resulting in severe drop in quality of service. There have been numerous admission control algorithms proposed. While some of these have been quite ingenious, there remains a great deal of room for improvement.

For example, Centinkaya and Knightly, in an article entitled "Egress Admission Control," IEEE Info Com 2000, describe a framework for scaleable quality of service provisioning in which admission control decisions are made at the egress routers based solely on aggregate measurements obtained at the egress router. They introduce a measurement-based service envelope as a way to adaptively describe the end-to-end service received by a traffic class.

The present invention is an improvement upon the above technique in which a measurement-based admission control algorithm is based on the global effective envelopes of an arriving traffic aggregate and upon the service curves of the corresponding departing traffic aggregate. The admission control algorithm is well adapted to a variety of different network models. Although the invention will be principally described in the context of a multi-router network, the concepts employed are equally applicable to autonomous network systems and even switching devices. In a switching device, for example, the switch hardware/software provides several input ports and output ports. The present invention may be used to control flow of traffic among these input and output ports. Therefore, the invention is applicable to "networks" of different

architectural granularities, ranging from single device switches to large, multiple device computer network domain.

For a more complete understanding of the invention, its objects and advantages, refer to the following description and to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a network diagram illustrating an exemplary end-to-end network model, useful in understanding the admission control algorithm of the present invention;

Figure 2 is a block diagram illustrating the pertinent parameters associated with arriving traffic and admitted traffic in a network;

Figure 3a is a flowchart diagram of the presently preferred admission control algorithm, illustrating global effective envelopes;

Figure 3b is a similar flowchart diagram of the presently preferred admission control algorithm, illustrating local effective envelopes;

Figure 4 is a graph illustrating the calculation of delay bound;

Figure 5 is a timing diagram illustrating an example of a measured time interval, where $T = 3\tau$ and $M = 2$;

Figure 6a and 6 b are graphs illustrating measured arriving traffic for time interval $k\tau$ 100 ms;

Figures 7a and 7b are graphs illustrating measured service envelope for time interval 100 ms;

Figures 8a, 8b and 8c are graphs of average link utilization as a function of delay bound for three different scenarios, for delay bound d 100 ms.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Figure. 1, an exemplary network is illustrated at **10**. Network **10** includes a plurality of edge routers, such as router **12** and router **14** that are in turn connected to a plurality of core routers **16**. For purposes of illustration, the edge router **12** serves as the ingress node **18** and edge router **14** serves as the egress node **20**. Arriving traffic enters through the ingress node and departing traffic leaves through the egress node, as illustrated.

For purposes of illustration the arriving aggregate traffic **22** comes from network **24** via edge router **26**. For purposes of illustration it will be assumed that the edge router **26** includes a traffic conditioner function **28**, limiting the flow of arriving aggregate traffic to within predefined bounds.

For purposes of illustration the departing aggregate traffic **30** exits edge router **14** and enters network **32**.

Network **10** implements an admission control function **34** which of the packets of arriving aggregate traffic **22** are admitted to the network **10** and which are blocked. The admission control function **34** may be localized in a single router, such as edge router **12**. Alternatively, the admission control function can be distributed across the network, with the function being performed by plural routers within the network **10**. In accordance with the invention the admission control function **34** implements an admission control algorithm that is based

upon the global effective envelope **36** of the arriving aggregate traffic **22** and upon the service curves **38** of the departing aggregate traffic **30**.

Figure 2 illustrates network **10** with the arriving traffic, admitted traffic and departing traffic being shown in greater detail. The figure introduces some of the terms that will be useful in understanding the presently preferred algorithm. The arriving traffic **22** is assumed to be supplied through a traffic conditioner or regulator **28**, which may be implemented at the ingress node **18** to enforce the arriving traffic to comply with the traffic specification submitted by the sender. The traffic conditioner or regulator may be modeled as a leaky bucket that provides a simple metering function. Alternatively, the traffic conditioner may provide more sophisticated traffic shaping functions where the temporal characteristics of a traffic class are selectively modified by delaying local packet forwarding.

Associated with arriving traffic **22** is a deterministic envelope **42**. The deterministic envelope may be characterized in terms of three variables: peak traffic rate, average traffic rate and burst size parameter. The arriving traffic also is assumed to have an associated quality of service requirement **44**. Typically each class of service would have its own quality of service requirement. Thus multiple QoS requirements are illustrated at **44** in Figure 2. The QoS requirements may be characterized by the following variables: probability of delay violation and delay bound.

The admitted traffic **46** may be differentiated from the arriving traffic, in that the admitted traffic has already passed the admission control point and is thus currently flowing in network **10**. When the admitted traffic **46** leaves network

10 it represents departing traffic **30**. The departing traffic **30** has associated with it a service curve or service envelope **48** that is measured by monitoring each packet's arrival time and departure time.

The admission control algorithm of the presently preferred embodiment uses the associated deterministic envelope **42** of the arriving traffic and the associated service envelope **48** of the departing traffic in making a decision whether to admit or deny arriving traffic to meet the desired QoS requirements. Figures 3a and 3b show the presently preferred algorithm in flowchart form. A more rigorous mathematical derivation of the preferred algorithm is presented below. The flowcharts of Figures 3a and 3b make reference to specific equations from the detailed mathematical derivation, where applicable. A discussion of the flowchart will be presented first, as a way of introducing the detailed mathematical derivation that follows. Specifically, Figure 3a applies to global effective envelopes; Figure 3b applies to local effective envelopes. The content of these two figures is similar; hence a detailed discussion of Figure 3a is presented below and may be considered applicable to Figure 3b, except where the mathematical derivation differs, as will be evident by comparing the Figures.

Referring to Figure 3a, the preferred algorithm begins at step **60** with a request to be admitted to the network. As part of the request, the incoming traffic submits its traffic characterization, which is expressed in terms of characterization parameters **62**. The specific parameters used by the presently preferred embodiment are:

- Deterministic Envelope $A_j^*(\tau)$;

- Quality of Service Requirements, QoS;
- Delay Bound, d;
- Probability of Delay Violation, ε.

Next, at step **64**, the algorithm constructs a global effective envelope for the arriving traffic, based on the submitted parameters **62**. In the mathematical derivation that follows, the effective envelope for arriving traffic is characterized as G_{new}. The G_{new} envelope is depicted in Figure 3 at **66**. As indicated by the dashed lines and bracketed notation, step **64** is performed using equations 3.8-3.11.

Next the algorithm continues at step **68** to construct a global effective envelope for the admitted traffic, based on measured statistics. Specifically, the measured statistics, listed at **70**, include the average and the variance of the amount of arriving aggregate traffic. In the detailed mathematical derivation which follows, the global effective envelope for admitted traffic is designated as $G^q_{N_q}$. In Figure 3, this $G^q_{N_q}$ envelope is shown at **72**.

The final admission control decision, step **74**, is made based on an analysis of both effective envelopes **66** and **72** along with the service curve **40** calculated using equation 4.5 and the algorithm shown in Table I below. Specifically, the admission control decision will admit incoming traffic if:

$$G_{new} + G^q_{N_q} \leq S^q$$

For a more precise statement of the above admission control condition, see the following detained description and in particular, Eqn. (3.12).

Detailed Description of Preferred Admission Control Algorithm

A detailed description of the preferred algorithm will now be provided below. For purposes of illustration a Differentiated Service (DS) or DifServ architecture will be assumed. The invention is not limited to the DS architecture inasmuch as the admission control algorithm of the invention may be used with a variety of network architectures.

In order to provide Quality of Service (QoS), the Integrated Services (IS) architecture use a signaling protocol to set up resource reservations at all routers along the path. Since this approach requires that all routers have to keep per-flow state and process the per-flow resource reservations, this approach has known scalability problems. Differentiated Service (DS) is another approach to provide QoS, but without the restriction on scalability. Routers need only to implement scheduling and buffering mechanisms and apply them based on the DS Code Point (DSCP) presented in the header of arriving packets. The end-to-end QoS service across several domains is built by combining the per domain behaviors (PDBs) of individual DS domains. Those PDBs in their terms are constructed by an appropriate deployment of per-hop forwarding behaviors (PHBs). Several DS domains can exist within a single autonomous system (AS). The definition of PDBs is an active area of research, with the first few drafts currently available]. Hence DS addresses scalability by providing QoS guarantees on traffic aggregate level.

As discussed above, one of the critical requirements for service provisioning across a DS domain is a presence of an effective Connection Admission Control (CAC). Such admission control can be utilized while establishing dynamic service level agreements (SLAs) for premium service across DS network, or consulted upon re-negotiations of static SLAs. Bandwidth Broker (BB) entity of a DS domain is a typical place for such admission control. The difficulty involved in designing the effective CAC, is that many solutions lead toward topology-dependent implementations, thus limiting their scope and increasing their complexity.

To implement admission control for DS without scalability problems, several researchers have proposed various forms of Endpoint CAC. In this design, the endpoints of a DS domain (ingress/egress routers) perform admission control and resource management. The routers measure traffic in the network to detect the level of available resources and admit a new connection if and only if, the detected level of resource is sufficiently high.

The preferred embodiment provides a measurement-based CAC algorithm, which provides statistical QoS guarantees on a traffic aggregate level in a DS domain. The ingress traffic arriving at the boundary of a DS domain is assumed to be conditioned by the upstream domains, policed by our domain to adhere to the rules of an established SLA, and further marked with the appropriate DSCP. Leaky-bucket based policers, shapers and markers are widely proposed. As the DS architecture extends some PDB for a traffic aggregate, we call this traffic aggregate a class in a subsequent discussion (different from DS class). We target the PDBs, which offer delay

guarantees to a classified traffic aggregate given both delay and delay violation probability. We described the deterministic envelopes, i.e., arriving traffic envelopes and service envelopes, and the bound on performance characteristics, which can be obtained, from those envelopes. We then derive a measurement-based CAC to establish dynamic SLA and provide statistical guarantees for a variety of service classes by exploiting the statistical traffic envelopes, called *global effective envelopes* and *service curves.* To obtain these envelopes, we use the measurement approach. The measurement of the service curves allows our admission control condition to work without the knowledge of the topology of the DS domain and cross traffic in the domain.

Let us consider a traffic arriving to a network domain. The traffic enters the domain at an ingress node **18** and destines to an egress node **20** (see Figure 1). In the following we consider a continuous-time fluid low traffic model. An arriving traffic from different flows is differentiated by its QoS requirements. Here we consider the probability of delay violation and the delay bound as the QoS requirements of interest. An arriving traffic with the same QoS requirements, i.e., the same delay bound and probability of delay violation requirements, is treated as a service class. Hence, arriving traffic into the domain is partitioned into Q classes. We use N_q to denote the number of flows within a class q.

The arriving traffic from the flow j of the class q in an interval (t_1, t_2) is denoted as $A_j^q(t_1, t_2)$. We assume that traffic arrival from each flow j is

regulated by a traffic conditioner and upper bounded by a deterministic subadditive envelope $A_j^{q*}(\tau)$ as follows:

$$A_j^q(t,t+\tau) \le A_j^{q*}(\tau) \qquad \forall t \ge 0,\ \forall \tau \ge 0. \tag{2.1}$$

The arriving traffic is characterized by the deterministic envelope with a set of parameters. The most commonly used traffic regulators are leaky buckets with a peak rate enforcer. The traffic on flow j is characterized then by three parameters (P_j, σ_j, ρ_j) with a deterministic envelope is given by

$$A_j^{q*}(\tau) = \min\{P_j^q \tau, \sigma_j^q + \rho_j^q \tau\} \qquad \forall \tau \ge 0 \tag{2.2}$$

where $P_j^q \ge \rho_j^q$ is the peak traffic rate, ρ_j^q is the average traffic rate, and σ_j^q is the burst size parameter.

As a generalization of the peak-rate enforced leaky bucket the traffic on flow j may be characterized by a set of parameters $\{\sigma_{jk}^q, \rho_{jk}^q\}_{k=1,\ldots,K_j}$, with a deterministic envelope

$$A_j^{q*}(\tau) = \min_{k=1,\ldots,K_j^q} \{\sigma_{jk}^q + \rho_{jk}^q \tau\} \tag{2.3}$$

where K_j^q is the number of leaky-bucket pairs.

It is also noted that flows from the same service class can be characterized by different deterministic envelopes, but can have the same QoS requirements.

We use $A_j^{qout}(t_1,t_2)$ to denote the traffic from flow j of the class q leaving the domain at the egress node in an interval (t_1,t_2). We then define the aggregate traffic of class q as follows: the aggregate of arriving traffic, $A_{Nq}(t_1,t_2) = \sum_{j \in Nq} A_j^q(t_1,t_2)$ and the aggregate of departing traffic

$A_{Nq}^{out}(t_1,t_2) = \sum_{j \in Nq} A_j^{qout}(t_1,t_2)$. For a time interval of length β, we define *the empirical envelope*, $E_{Nq}(\tau;\beta)$ of an arriving aggregate N_q of flows from class q, which is the upper bound of the arriving aggregate in any time interval of length $\tau \leq \beta$ as follows:

$$E_{Nq}(\tau;\beta) = \sup_{(t,t+\tau)\subseteq\beta} A_{Nq}(t,t+\tau) \tag{2.4}$$

In the following, we will focus our discussion on the aggregate traffic of a single service class and drop the index 'q'. We will introduce the definition of a service curve and its application. We assume that there is no traffic in the domain at time $t=0$. Therefore, for an aggregate traffic, the amount of backlogged traffic in the domain at any time t, $B(t)$, is given by

$$B(t) = A_N(0,t) - A_N^{out}(0,t) \geq 0. \tag{2.5}$$

Also the ingress-to-egress delay suffered by the aggregate traffic at time t is denoted by $d(t)$ and is defined as follows:

$$d(t) = \min\{z : z \geq 0 \text{ and } A_N(0,t) \leq A_N^{out}(0,t+z)\} \tag{2.6}$$

Definition of Service Curve

Let $S(\cdot)$ be a non-decreasing function, with $S(0)=0$. We say that the domain guarantees the service curve $S(\cdot)$ for the aggregate traffic if for any time t, there exists $s \le t$ such that $B(s)=0$ and $A_N^{out}(s,t) \ge S(t-s)$.

It can be seen that $S(t-s)$ specifies the lower bound of the amount of the aggregate traffic needed to be served and depart from the domain during some interval (s,t), where the domain is empty at time s.

From the definition of service curve, the upper bound of delay can be obtained as follows. Consider a busy period of length β. Let s denote the starting time of the busy period, that is, $B(s)=0$ and $A_N(0,s)=A_N^{out}(0,s)$. We assume that the domain guarantees the service curve $S(\cdot)$, that is $A_N^{out}(s,t) \ge S(t-s)$, where $s \le t+d \le \beta$. From the definition of service curve, we have $A_N^{out}(s,t+d)=A_N^{out}(0,t+d)-A_N(0,s) \ge S(t+d-s)$. From Eqn. (2.6), thus, $A_N(0,t) \ge A_N^{out}(0,t+d) \ge A_N(0,s)+S(t+d-s)$. Hence, from Eqn. (2.4),

$$A_N(s,t) \le E_N(t-s;\beta) \ge S(t+d-s) \tag{2.7}$$

Let $\tau = t-s$, it then follows that, for all time $t \ge 0$, the delay defined in Eqn. (2.6) is upper bounded as follows:

$$\begin{aligned} d(t) &\le \min\{z : z \ge 0 \text{ and } E_N(\tau;\beta) \le S(\tau+z)\} \\ &\le \max_{0\le\tau\le B} \min\{z : z \ge 0 \text{ and } E_N(\tau;\beta) \le S(\tau+z)\} \end{aligned} \tag{2.8}$$

From Eqn. (2.8), it is note that the upper bound on delay is the maximum horizontal distance between the arriving aggregate envelope ($E_N(\tau;\beta)$) and the

service curve $S(\tau)$ (see Figure 4). It is also noted that β is upper bounded by $\beta_{\max}$, which is the maximum busy period of the aggregate traffic and can be determined as: $\beta_{\max} = \inf\{\tau \geq 0 | \sum_{j \in N} A_j^*(\tau) \leq S(\tau)\}$. Therefore, we will use $\beta = \beta_{\max}$ in the following discussions.

The preferred admission control algorithm exploits the deterministic envelopes and the service envelopes to obtain the upper bound of the delay experienced by an arriving traffic based on the worst-case scenario where it is assumed that all flows send traffic with their peak rate simultaneously.

In the next section, following the concept of the described envelopes, we will derive a statistical service where a small portion of traffic is allowed to violate the delay QoS requirement. We will use so called global effective envelopes to characterize arriving aggregate traffic for each class. Using these envelopes allows us to derive a CAC for statistical services which can be perform the same fashion as for deterministic services.

Probabilistic Guarantees with Effective Envelopes and Service Curves

In this section, we derive the probability of delay violation based on the upper bound of the delay shown in the previous section. We then obtain an admission control condition for a single service class by applying the definition of local and global effective envelope presented in R. Boorstyn, A. Burchard, J. Liebeherr, and C. Oottamakorn. Effective envelopes: Statistical bounds on multiplexed traffic in packet networks. In *Proceedings of IEEE INFO COMM*

2000, Tel Aviv, Israel, March 2000 (hereinafter "Boorstyn, et. al."). We finally discuss the admission control conditions for multiple service classes.

Probabilistic Guarantees with local Effective envelopes and Service Curves

Again we will first consider a single service class and we drop the index 'q'. An aggregate of arriving traffic from the same service class $A_N(t_1,t_2)$ has the same probability of delay violation, ε, and delay bound requirement, d. $A_N(t_1,t_2)$ are upper bounded by a family of nonnegative random processes $A_N(t_1,t_2)$, which has the following properties: (1) Stationarity: the statistical properties of $A_N(t_1,t_2)$ do not change with time (2) Independence: The $A_N(t_1,t_2)$ are stochastically independent among all service classes. Let again $D_N(\tau)$ denote the ingress-to-egress delay experienced by a bit of an aggregate traffic of the N flows which arriving at the domain at time τ. We assume that $D_N(\tau)$ is a random variable. For a given delay bound d, the domain guarantees that the ingress-to-egress delay of any arriving bit will not exceed the delay bound d, that is, for all time $t \geq 0, 0 \leq \tau \leq B_{\max}$, from Eqn. (2.8), $D_N(\tau) = \min\{z : z \geq 0$ and $A_N(t,t+\tau) \leq S(\tau+z)\} \leq d$ or, for all time $t \geq 0$, $0 \leq \tau \leq B_{\max}$, $A_N(t,t+\tau) \leq S(\tau+d)$. The delay violation occurs if $\exists D_N(\tau)$ such that

$$D_N(\tau) \geq d$$

or, $\exists \tau$ such that

$$A_N(t,t+\tau) > S(\tau+d)$$

With Eqn. (2.8), the probability that the arriving traffic experiences a delay violation is required to be bounded by ε and we have, for all time $t \geq 0$, $0 \leq \tau \leq B_{\max}$,

$$\Pr[D_N(\tau) > d] = \Pr[A_N(t, t+\tau) > S(t+d)] \leq \varepsilon \quad (1)$$

A set of new flows request same service guarantees from a DS domain. The CAC uses the admission control test to ensure that the requested service guarantees and other flows from all service classes can be simultaneously satisfied. From Eqn. (1), we can obtain the admission control condition for a single service class by using the definition of local effective envelope as follows:

Definition (Local Effective Envelope)

A local effective envelope for $A_N(t, t+\tau)$ is a function L_N that satisfies for all $\tau \geq 0$ and all t

$$\Pr[A_N(t, t+\tau) \leq L_N(\tau; \varepsilon)] \geq 1 - \varepsilon$$

It can be seen that a local effective envelope provides a probabilistic bound for the aggregate traffic $A_N(t, t+\tau)$ for any specific time interval of length τ.

Lemma

Given a set of flows that is partitioned into M classes, and each class contains N_m flows with aggregate arrivals, A_{N_m}. Let $L_{N_m}(\tau;\varepsilon)$ be local effective envelope for class m. Then the following inequality holds: given x,

$$\text{If } \sum_m L_{N_m}(\tau;\varepsilon) \le x, \text{ then for all } t, \Pr\left[\sum_m A_{N_m}(t,t+\tau) > x\right] \le M \cdot \varepsilon.$$

We divide flows from the same service class into two categories, i.e. $M = 2$. The first group is the set of flows, N that are already admitted to the domain. The second group is the new set of flows, K, requesting the QoS service from a DS domain. We denote L_N as the local effective envelope of the first group and L_{new} as the local effective envelope of the second group.

Admission control condition for a single service class

From the definition of the local effective envelope and the lemma, from Eqn. (1), we have that the arriving traffic has a delay violation with probability $< \varepsilon$ if

$$L_N(\tau;\varepsilon/2) + L_{new}(\tau;\varepsilon/2) \le S(\tau+d) \quad \text{, for } 0 \le \tau \le B_{\max} \qquad (2)$$

Remark:

- If for the same service class the set of new flows are regulated by different deterministic envelopes A_j^*, for each set of flows which have the same A_j^* it is required to construct their $L_{new}^j(\cdot;\varepsilon_j)$, where $\sum_j \varepsilon_j = \varepsilon/2$. Therefore Eqn. (2) becomes

$$L_N(\tau;\varepsilon/2) + \sum_j L_{new}^j(\tau;\varepsilon_j) \le S(\tau+d) \quad \text{, for } 0 \le \tau \le B_{\max} \qquad (3)$$

- The CAC in Eqn. (2) does not depend on the topology of the domain and the scheduling algorithms within the domain, but the measurement-based traffic-characterized envelopes, which can be measured at an ingress and egress node in a DS domain.

Local Effective Envelope using Measured Moment

We consider a set of admitted flows, N. We characterize the distribution of the aggregate traffic using the Central Limit theorem, which does not require the knowledge of the underlying distributions of each flow. An approximate local effective envelope of the aggregate traffic can be obtained from the Central Limit Theorem as follows [1]. From the definition of the local effective envelope, we set $\Pr[A_N(t,t+\tau) \geq x] \approx \varepsilon/2$ and we obtain,

$$L_N(\tau;\varepsilon/2) \approx \overline{X(\tau)} + z\sigma(\tau) \qquad (4)$$

where z has the approximate value $z \approx \sqrt{|\log(2\pi\varepsilon)|}$, and $\overline{X(\tau)}$ and $\sigma^2(\tau)$ are measured average and variance of the amount of aggregate traffic, respectively. We will discuss those measurements in the next section.

Since the number of new flows may be just a few flows, the Central Limit theorem may not be the appropriate choice for constructing their local effective envelope, i.e., the bound obtained may not be tight enough. Instead, we will use the Chernoff bound, which provides more rigorous bound on the aggregate traffic. The local effective envelope of a set of

new flows, K, can then be obtained by using the Chernoff bound, and is given as follows:

Recall the Chernoff bound for a random variable Y:

$$\Pr[Y \geq y] \leq e^{-sy} \mathrm{E}[e^{sy}] \qquad \forall s \geq 0 \tag{5}$$

We have

$$\Pr[A_K(t, t+\tau) \geq Kx] \leq e^{-Kxs} \mathrm{M}_K(s, \tau). \tag{6}$$

where $\mathrm{M}_K(s, \tau)$ is the moment generating function of the aggregate traffic.

In Boorstyn, et. al. $\mathrm{M}_K(s, \tau)$ is derived and given in term of the deterministic envelopes of the flows, that is the leaky bucket function in our case. s is chosen so that Eqn. (6) is minimal. With these values of s and $\mathrm{M}_K(s, \tau)$, it yields

$$L_{new}(\tau; \varepsilon/2) = K \min\{x, A_K^*(\tau)\} \tag{7}$$

$$\left(\frac{\rho\tau}{x}\right)^{\frac{x}{A_K^*(\tau)}} \left(\frac{A_K^*(\tau) - \rho\tau}{A_K^*(\tau) - x}\right)^{1-\frac{x}{A_K^*(\tau)}} \leq (\varepsilon/2)^{1/K} \tag{8}$$

where $A_K^*(\tau)$ is a deterministic envelope for each new flow.

Admission control condition for multiple service classes

The admission control condition in Eqn. (2) does not provide the guarantee that QoS requirements of other service classes use the same ingress-to-egress path will be satisfied if a new set of flows is admitted into the domain. To be able to provide their guarantees, without loss of generality, we assume that the new flows have the highest priority and we test the admission control condition for all the service classes. This can

be shown as follows. For each service class we obtain an arriving aggregate traffic envelope $L^q_{N_q}(\tau;\varepsilon_q/2)$ and a service envelope $S^q(\cdot)$. From Eqn. (2), the new flows with an arriving envelope $L_{new}(\tau;\varepsilon_q/2)$ will be admitted if the following condition is satisfied: for all service classes q,

$$L^q_{N_q}(\tau;\varepsilon_q/2)+L_{new}(\tau;\varepsilon_q/2)\le S^q(\tau+d_q) \quad \text{, for } 0\le\tau\le B_{\max} \tag{9}$$

In this section we show our CAC, which depends on the measurement-based envelopes ($L_N(\cdot;\varepsilon)$ and $S(\cdot)$). In the next section we show how to obtain these envelopes.

Probabilistic Guarantees with Global Effective envelopes and Service Curves

In this section, we derive the probability of delay violation based on the upper bound of the delay shown in the previous section. We then obtain an admission control condition for a single service class by applying the definition of global effective envelope presented in. We finally discuss the admission control conditions for multiple service classes.

Again we will first consider a single service class and we drop the index 'q'. An aggregate of arriving traffic from the same service class in the interval (t_1,t_2), $A_N(t_1,t_2)$ has the same QoS requirements: probability of delay violation, ε, and delay bound requirement, d. $A_N(t_1,t_2)$ is characterized by a family of nonnegative random processes, which has the following properties: (1) Stationarity: the statistical properties of $A_N(t_1,t_2)$ do not change with time (2) Independence: The $A_N(t_1,t_2)$ are stochastically independent among all service

classes. Consider an interval of length of the maximum busy period β. Let again $D_N(t)$ denote the ingress-to-egress delay experienced by a bit of an aggregate traffic of the N flows which arriving at the domain at time t during the busy period. We assume that $D_N(t)$ is a random variable. For a given delay bound d, the domain guarantees that the ingress-to-egress delay of any arriving bit will not exceed the delay bound d, that is, from Eqn. (2.8), for all τ, $0 \le \tau \le \beta$,

$$D_N(t) = \min\{z : z \ge 0 \text{ and } \sup_{(t,t+\tau)\subseteq\beta} A_N(t,t+\tau) \le S(\tau+z)\} \le d \qquad (3.1)$$

or, for all τ, $0 \le \tau \le \beta$,

$$\sup_{(t,t+\tau)\subseteq\beta} A_N(t,t+\tau) = E_N(\tau;\beta) \le S(\tau+d). \qquad (3.2)$$

The delay violation occurs if $\exists D_N(t)$ such that

$$D_N(t) \ge d$$

or, $\exists t, \tau$ such that

$$\sup_{(t,t+\tau)\subseteq\beta} A_N(t,t+\tau) > S(\tau+d)$$

With Eqn. (3.2), the probability that the arriving traffic experiences the delay violation is required to be bounded by ε and we then have

$$\Pr[D_N(t) \le d, \forall t, \tau] = \Pr[E_N(\tau;\beta) \le S(t+d), \text{for all } \tau, 0 \le \tau \le \beta]$$

$$\leq \quad 1-\varepsilon \tag{3.4}$$

A set of new flows request same service guarantees from a DS domain. The CAC uses the admission control test to ensure that the requested service guarantees and other flows from all service classes can be simultaneously satisfied. From Eqn. (3.4), we can obtain the admission control condition for a single service class by using the definition of global effective envelope as follows:

Definition of Global Effective Envelope

A global effective envelope for an interval of length β is a subadditive function $G_N(\tau;\beta,\varepsilon)$ that satisfies:

$$\Pr\left[E_N(\tau;\beta) \leq G_N(\tau;\beta,\varepsilon), \forall 0 \leq \tau \leq \beta\right] \geq 1-\varepsilon$$

It can be seen that a global effective envelope provides a probabilistic bound for the aggregate traffic $A_N(t,t+\tau)$ for every time interval of length τ in β.

Lemma

Given a set of flows that is partitioned into M classes, and each class contains N_m flows with aggregate arrivals, A_{N_m}. Let $G_{N_m}(\tau;\beta,\varepsilon)$ be global effective envelope for class m. Then the following inequality holds: given x,

If $\sum_m G_{N_m}(\tau;\beta,\varepsilon) \le x$, then for all t, $\Pr\left[\exists m \exists \tau : \sum_m E_{N_m}(t,t+\tau) > x(\tau)\right] \le M \cdot \varepsilon$.

We divide flows from the same service class into two categories, i.e. $M = 2$. The first group is the set of flows, N that are already admitted to the domain. The second group is the new set of flows, K, requesting the QoS from a DS domain. We denote G_N as the global effective envelope of the first group and G_{new} as the global effective envelope of the second group.

Admission Control Condition for a Single Service Class

From the definition of the global effective envelope and the lemma, from Eqn. (3.4), we have that the arriving traffic has a delay violation with probability $< \varepsilon$ if

$$G_N(\tau;\beta,\varepsilon/2) + G_{new}(\tau;\beta,\varepsilon/2) \le S(\tau+d) \quad \text{, for } 0 \le \tau \le B \qquad (3.5)$$

Remark:

- If for the same service class the set of new flows are regulated by different deterministic envelopes A_j^*, for each set of flows which have the same A_j^* it is required to construct their $G_{new}^j(\cdot;\beta,\varepsilon_j)$, where $\sum_j \varepsilon_j = \varepsilon/2$. Therefore Eqn. (3.5) becomes:

$$G_N(\tau;\beta,\varepsilon/2) + \sum_j G_{new}^j(\tau;\beta,\varepsilon_j) \le S(\tau+d) \quad \text{, for } 0 \le \tau \le B \qquad (3.6)$$

- The CAC in Eqn. (3.5) does not depend on the topology of the domain and the scheduling algorithms within the domain, but the measurement-based traffic-characterized envelopes, which can be measured at an ingress and egress node in a DS domain.

Constructing the Global Effective Envelope

We consider a set of admitted flows, N. We characterize the distribution of the aggregate traffic using the Central Limit theorem, which does not require the knowledge of the underlying distributions of each flow. An approximate

global effective envelope $G_N(\tau;\beta,\varepsilon)$ of the aggregate traffic can be obtained from the Central Limit Theorem as follows. From the definition of the global effective envelope, we set $\Pr[E_N(\tau;\beta) \geq x, \quad \forall 0 \leq \tau \leq \beta] \approx \varepsilon$. For given τ_0, β we then have, for every integer k,

$$G_N(\tau;\beta,\varepsilon) \approx \alpha[\overline{X((k+1)\tau/k)} + z'\sigma((k+1)\tau/k)], \quad \forall \tau \in [\tau_0, \beta] \tag{3.7}$$

where $\alpha = 1+1/(k+1)$, z' has the approximate value $z' \approx \sqrt{|\log(2\pi\varepsilon')|}$ with $\varepsilon' = \tau_0(\alpha-1)\varepsilon/\beta k$, $\overline{X(\tau)}$ and $\sigma^2(\tau)$ are measured average and variance of the amount of aggregate traffic, respectively. We will discuss those measurements in the next section.

From Eqn. (3.4) it can be seen that there are several possible global effective envelopes. For given τ_0, β, the method recursively calculate the $k_i, \alpha_i, \text{and } \tau_i$ for $1 \leq i \leq n$, where τ_n is the first point which is greater than β, therefore we can obtain n points of a global effective envelope as follows:

$$k_i = z\left(z + \frac{\overline{X(\tau_{i-1})}}{\sigma(\tau_{i-1})}\right), \tag{3.8}$$

$$\alpha_i = 1 + \frac{1}{k_i + 1}, \tag{3.9}$$

$$\tau_i = \alpha_i \tau_{i-1}, \tag{3.10}$$

and, from Eqn. (3.7),

$$G_N(\tau_i;\beta,\varepsilon) \approx \alpha_i[\overline{X((k_i+1)\tau_i/k_i)} + z'\sigma((k_i+1)\tau_i/k_i)] \quad (3.11)$$

where $z \approx \sqrt{|\log(2\pi\varepsilon)|}$.

For a set of new flows, one can obtain the global effective envelope of the new flows G_{new} by using the same recursive method as follows. However, instead of using the measurement-based $\overline{X(\tau)}$ and $\sigma^2(\tau)$, in Eqs. (3.8) and (3.11) $\overline{X(\tau)} = K\rho_K\tau$ and $\sigma^2(\tau) = K\rho_K\tau(A_K^*(\tau) - \rho_K\tau)$, where ρ_K is the long-term average and $A_K^*(\tau)$ is a deterministic envelope for each new flow.

Admission Control Condition for Multiple Service Classes

The admission control condition in Eqn. (3.2) does not provide the guarantee that QoS requirements of other service classes use the same ingress-to-egress path will be satisfied if a new set of flows is admitted into the domain. To be able to provide their guarantees, without loss of generality, we assume that the new flows have the highest priority and we test the admission control condition for all the service classes. This can be shown as follows. For each service class we obtain an arriving aggregate traffic envelope $G_{N_q}^q(\tau;\beta,\varepsilon_q/2)$ and a service envelope $S^q(\cdot)$. From Eqn. (3.5), the new flows with an arriving envelope $G_{new}(\tau;\beta,\varepsilon_q/2)$ will be admitted if the following condition is satisfied: for all service classes q,

$$G_{N_q}^q(\tau;\beta,\varepsilon_q/2) + G_{new}(\tau;\beta,\varepsilon_q/2) \le S^q(\tau+d_q) \quad \text{, for } 0 \le \tau \le B \quad (3.12)$$

In this section we show our CAC, which depends on the measurement-based envelopes ($G_N(\cdot;\beta,\varepsilon)$ and $S(\cdot)$). In the next section we show how to obtain these envelopes.

Measurements of Perspective Envelopes

In this section, based on, we show how to measure the characteristic parameters for constructing the global effective envelopes of the arriving aggregate traffic and the service envelope of the departing aggregate traffic for a single service class. First we measure the average and variance of the amount of arriving aggregate traffic, which are used in Eqn. (3.3). We then measure the service envelope of a single service class traffic. At the end of this section we show the admission control algorithm that we will use in the evaluation example below.

Measurement of Aggregate Arriving Envelopes

We are interested in the aggregate characteristic of an arriving traffic at ingress node. To characterize the aggregate traffic as a Gaussian process, we need to measure the first and second moment of the amount of traffic arriving at the ingress node. We note that in, the average and variance of arriving traffic rate are measured, while here we measure the average and the variance of the amount of an arriving traffic. Again let $A_N(t_1,t_2)$ denote the arriving traffic from an aggregate flow in the interval (t_1,t_2). Consider time to be slotted with the

equal length τ, i.e., for MPEG sources, we can think of τ as the frame time. We also divide time into M large intervals whose length is T (see Figure 5). For the m^{th} interval we obtain the bound of an arriving traffic, X_k^m as a function of time interval $k\tau$. We consider at the current time t. Then the bounded amount of the measured traffic over the m^{th} interval of length T from the current time can be obtained as follows:

$$X_k^m = \max_{0 \le n \le \left(\frac{T}{\tau} - k\right)} A[t - mT + n\tau, t - mT + (n+k)\tau] \tag{4.1}$$

for $m = 1, \ldots, M$ and $k = 1, \ldots, \frac{T}{\tau}$.

Thus for every T time slot, the bounded envelope X_k^m is obtained. From these envelopes we can obtain the average $\overline{X_k}$ and the variance σ_k^2 of the measured envelopes as follows:

$$\overline{X}_k = \sum_{m=1}^{M} X_k^m \tag{4.2}$$

and

$$\sigma_k^2 = \frac{1}{M-1} \sum_{m=1}^{M} (X_k^m - \overline{X}_k)^2 \tag{4.3}$$

Remark: τ, T, and M are the key parameters for the measurement. Choosing an improper choice of τ, T, and M may lead to inaccurately characterize the arriving aggregate traffic and consequently overestimate the bandwidth required

by connections. We varied these parameters in our approach and found that our approach is not very sensitive to the changing. The further discussion of how to choose the parameters can be found in C. Cetinkaya and E. Knightly. Egress Admission Control. In *Proceedings of IEEE INFO COMM 2000*, Tel Aviv, Israel, March 2000; and D. Tse and M. Grossglauser. Measurement-Based Call Admission Control: Analysis and Simulation. In *Proceedings of IEEE INFOCOM 1997*, Kobe, Japan, April 1997.

We provide an example of an arrival envelope from a simulation experiment in Figure 6(a) and (b). In Figure 6(a), we plot the amount of arrival aggregate traffic as a function of time interval. While Figure 6(b) depicts the arrival aggregate rate as a function of time interval. The simulation consists of 120 multiplexed independent MPEG-2 video traces. These traces are obtained from the movie "Starship Troopers" ("*Starship*"). *Starship* has the peak rate of 18.6336 Mbps and the average rate of 4.26 Mbps. The frame rate of *Starship* is 30 frames per second. This type of traffic has a quite large peak-to-mean ratio, which indicates its significant burstiness. From Figure 6, the arriving envelope and arrival rate are significantly smaller than the peak envelope and peak rate, respectively. This is due to the statistical multiplexing of the traffic aggregate. As the figures show, given a long time interval, the amount of the arriving traffic and its arrival rate decrease toward the average rate.

Measurement of Aggregate Service Envelopes

Consider traffic arriving at a DS domain at an ingress node and leaving at an egress node. For measuring service envelopes, we assume that the clocks in

the domain are synchronized. We consider at the packet system where packets are serviced at discrete times rather than continuous times. Each packet arriving at the ingress node will be time-stamped. Hence at the egress node, we are able to determine the ingress-to-egress delay of each packet. Let a_j denote the arriving time and d_j denote the departure time of the j^{th} packet. We consider this traffic to be backlogged whenever at least one packet in the system. The backlogging condition can be checked by comparing the arriving and the departure times of packets. Traffic is continuously backlogged for k packets in the interval $[a_j, d_{j+k-1}]$ if

$$d_{j+m} > a_{j+m+1} \quad \text{, for all } 0 \le m \le k-2 \qquad (4.4)$$

for $k \ge 1$.

Next, let *ServEnv* is a list containing $(x, S_j^k(x))$ pairs which represent the amount of time $S_j^k(x)$ required to service *x* bits when considering the packet *j* with the number of backlogged packets = *k*. Again consider an interval of length *T*, which contains the total number of arriving packets, *n*. For packet *j*, we consider the delay of the packet and also the delay of the packets backlogged after this packet. We thus can define $S_j^k(x)$ as follows:

$$S_j^k(x) = d_{j+k-1} - a_j \qquad (4.5)$$

for all $k \ge 1$ and satisfies the backlogging condition.

A bounded service envelope can be obtained as follows:

Initialize (*ServEnv*)
for packet $j = 1$ to n
$S_j^1 <- d_j - a_j$
$x(S_j^1) <-$ Size (packet (j))
$k <- 2$
while ($d_{j+k-2} > a_{j+k-1}$)
$S_j^k <- d_{j+k-1} - a_j$
$x(S_j^k) <- x(S_j^{k-1})$ + Size (packet ($j+k-1$))
$k <- k + 1$
Merge (*ServEnv*, ($x(S_j^k)$, S_j^k) $\forall k$, *ServEnv*)
for i = (Length(*ServEnv*) -1) to 0
if ($x[i] < x[i-1]$)
Remove ($x[i-1], S[i-1]$)
Using *ServEnv* to plot a service envelope.

Table I Bounded Service Envelope Algorithm

Figure 7(a) shows a service envelope of an aggregate of departing traffic obtained from a simulation. The simulation consists of a node with a 622-Mbps link and the same number of sources (*Starship*) used for Figure 6a and 6b. It is noted that the envelope is an increasing function. In addition, Figure 7(b) depicts the slope of the service envelope. The slope of the envelope indicates variation of the service rate for the burstiness of the arriving aggregate flows.

Admission Control Algorithm using local effective envelopes

I. To request the QoS for its traffic from a DS domain, the user submits to a BB its traffic characterization containing $A_j^*(\tau)$, QoS requirements, d and ε.

II. CAC constructs a local effective envelope, L_{new}, based on the submitted parameters by using Eqs. (7) and (8).

III. CAC then uses the measurement of the average and variance of arriving traffic to construct another local effective envelopes, $L^q_{N_q}$, from Eqn. (4).

IV. CAC finally makes an admission control decision based on L_{new}, $L^q_{N_q}$, and S^q obtained from Section as follows. The request is accepted if the condition in Eqn. (9) is true.

Admission Control Algorithm using Global Effective Envelope

I. To request the QoS for its traffic from a DS domain, the user submits to a BB its traffic characterization containing $A^*_j(\tau)$, QoS requirements, d and ε.

II. CAC constructs a global effective envelope, G_{new}, based on the submitted parameters by using Eqs. (3.8) – (3.11).

III. CAC then uses the measurement of the average and variance of arriving traffic (obtained from Eqs. (4.2) and (4.3) respectively) to construct another global effective envelopes for admitted flows, $G^q_{N_q}$, from Eqs. (3.8)-(3.11).

IV. CAC finally makes an admission control decision based on G_{new}, $G^q_{N_q}$, and S^q obtained from Section as follows. The request is accepted if the condition in Eqn. (3.12) is true.

Evaluation and Simulation Results

In this section, we evaluate the effectiveness of our CAC condition. We consider that all flows are homogeneous, that is, all flows satisfy the same deterministic envelope and require the same delay QoS guarantee from a DS domain. *Starship* is again used as a traffic source. For simulations, we set the probability of delay violation $\varepsilon = 10^{-6}$ and vary the delay bound requirement d. We consider a DS domain, which has an egress node with a link capacity of 622 Mbps ($C =$ 622 Mbps for all simulations). All links in the domain has the same capacity as of the egress link. Each node has a FIFO scheduler. We consider three scenarios where the number of nodes and cross traffic in the domain is changed as follows:

I. The DS domain consists of a node without any cross traffic (see Figure 8(a)).
II. The DS domain consists of two nodes without any cross traffic (see Figure 8(b)).
III. The DS domain consists of three nodes with some cross traffic (see Figure 8(c)).

Note that in configuration III, we also use 40 flows of *Starship* as cross traffic with the same QoS requirements as of the main traffic.

We will evaluate our approach ('Approach') by using the CAC algorithm described above. As the benchmarks for our approach, we also investigate two of the following approaches and a set of simulations ('Simulation'). First, we

consider average rate allocation ('Average Rate'), where the maximum number of admissible flows is determined by the link capacity divided by the long-term average rate of each flow and, therefore, the average link utilization for this approach is unity. Second, we consider the peak rate allocation ('Peak Rate'), where the maximum number of admissible flows is determined by the link capacity divided by the peak rate of each flow. For the simulation proposes, each flow starts randomly sending traffic into the DS domain. Many simulations are performed. The average result of the simulation is presented. We compare the average link utilization, U_{ave}, obtained from each approach. U_{ave} is defined as follows:

$$U_{ave} = \frac{\sum_{j=1}^{N} \rho_j}{C}$$

where N is the number of connection admitted to the domain, ρ_j is the long-term average rate of each flow, and C is the link capacity at the egress node.

Figures 8a-8c show the three scenarios we investigate and the corresponding results where the average link utilization as a function of the delay bound is depicted. From the results, the link utilization obtained by the simulations and our approach is considerably higher than the one obtained by the peak rate allocation. This shows that the simulations and our approach can exploit the multiplexing gain from the traffic aggregate and, hence, yield the high link utilization. For example, from Fig 8(a), for the delay bound d = 10 msec, the simulation and our approach yield 86% of the link utilization, respectively. While the peak rate allocation can only obtain 82%. In addition, the results show that

our approach can accurately characterize arriving and departing aggregate traffic. Figures 8(b)-(c) show that our approach can obtain the accurate condition of the domain without the knowledge of the underlying topology and cross traffic and yield the link utilization close to the simulation results.

From the foregoing it will be appreciated that the present invention provides a measurement-based admission control algorithm that exploits the global effective envelopes and service envelopes to accurately characterize arriving and departing traffic aggregate. Based on the measurement, the CAC algorithm is tunable through a set of parameters. The algorithm is scalable and can support a variety of service classes. We showed the effectiveness of the CAC algorithm by comparing the link utilization obtained by the algorithm to the results from the simulations. While the invention has been described in its presently preferred form, it will be understood that the principles of the invention may be applied to may application and that implementation details of the algorithm can be varied without departing from the spirit of the invention as set forth in the appended claims.